

Type of Submission: Paper

XP-001031568

P.D.	1840/1999
P.	97-M 15

Title or Topic: The Network Vulnerability Tool (NVT) –  
A System Vulnerability Visualization Architecture

**Abstract:** For the past two years, Harris Corporation has been conducting research for the U.S. Air Force Research Laboratory under the Network Vulnerability Tool (NVT) Study. The Network Vulnerability Tool concept develops and applies a single topological system model. This model supports the information needs of multiple vulnerability analysis tools using an integrated knowledge solicitation and translation framework. As part of this effort, vulnerability tools from COTS, GOTS, and research laboratory sources were surveyed, and a representative sample tool collection was selected for inclusion in the NVT prototype. The prototype integrates and interactively applies multiple existing vulnerability assessment technologies, resulting in a cohesive, combined vulnerability/risk assessment. The combined risk assessment provides a readily comprehensible picture of the risk posture, assisting the analyst in the definition of an acceptable risk posture for an operational system or preliminary system design. The NVT program has defined and developed a vulnerability assessment environment, consolidating multiple vulnerability sources and tools types into a coherent vulnerability visualization architecture. This paper describes the Network Vulnerability Tool architecture, its components, important architecture features, benefits of the NVT approach, and potential future enhancements.

**Keywords:** Vulnerability Assessment, Risk Management, Data Visualization, Security Architecture and Design

**Authors:** Ronda R. Henning and Kevin L. Fox, Ph.D.

**Organizational Affiliation:** Harris Corporation

**Telephone Numbers:** 407-984-6009 (voice)  
407-984-6353 (fax)

**E-mail address:** [rlenning@harris.com](mailto:rlenning@harris.com)

**Point of Contact:** Ronda Henning

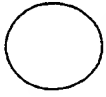
**U.S. Government Program Sponsor:** Air Force Research Laboratory/IFGB

**Contract Number:** F30602-96-C-0289

**U.S. Government Publication Release Authority:** Dwayne P. Allain or Peter J. Radesi

CITED H #6879, 605D 1077 COUNTRY W0

# The Network Vulnerability Tool (NVT) - A System Vulnerability Visualization Architecture

P.D. ....	
P. ....	

Ronda R. Henning  
Harris Corporation  
P.O. Box 98000, M/S W2-7756  
Melbourne, FL 32902  
(407) 984-6009  
[rhenning@harris.com](mailto:rhenning@harris.com)

Kevin L. Fox, Ph.D.  
Harris Corporation  
P.O. Box 98000, M/S W3-7755  
Melbourne, FL 32902  
(407) 984-6011  
[kfox@harris.com](mailto:kfox@harris.com)

## I. Introduction

The next generation of information systems and infrastructures under development by the Department of Defense and the Intelligence Community are built upon the concept of acceptable risk. That is, the security features and system architecture are deemed to provide sufficient protection over the life of the data processed. In previous generations of systems a risk adverse vulnerability posture dictated custom hardware and software solutions. Today, the rapid evolution of technology and proliferation of computing power mandate the use of commodity Commercial-Off-The-Shelf (COTS) hardware and software components for cost effective solutions. This strong dependence on COTS implies that commercial grade security mechanisms are sufficient for most applications. Security architectures, therefore, must be structured to build operational, mission-critical systems with relatively weak COTS components. Higher assurance components are placed at community or information boundaries, forming an enclave-based security architecture that implements a defense-in-depth approach to information assurance.

There are few design tools available to the system architect to assist in maximizing the available protection mechanisms while remaining within the development budget. Current generation risk analysis tools usually are single vendor solutions that address a particular aspect or aspects of risk. These tools tend to fall into one of three categories:

1. Tools that work from documented vulnerability databases and possibly repair known vulnerabilities. Tools of this type are vendor-dependent for database updates, either through new product versions or by a subscription service. Examples from this category include ISS' Internet Scanner, Network Associates, Inc.'s CyberCop, and Harris' STAT.
2. Monolithic tools that use various parameters to calculate a risk indicator. These tools are difficult to maintain and hard to keep current with the rapidly evolving threat and technology environment. An example of this tool category is Los Alamos Vulnerability Assessment (LAVA) tool.
3. Tools that examine a particular aspect of the system, such as the operating system or database management system, but ignore the other system components. SATAN, for example, analyzes operating system vulnerabilities but ignores infrastructure components such as routers.

None of these tools implement an aggregate snapshot approach to the system, with a "drill down" or layered approach to facilitate addressing risk at various layers (network, platform, database, etc.) of the system. They provide little assistance to system designers when analyzing alternatives among security risk, system performance and mission functionality. Instead, a "risk solution" is provided that addresses the particular aspect of risk that a given tool was designed to calculate. To develop a comprehensive risk assessment, a tool

user would have to become proficient in the use of several tools, and manually correlate the resulting outputs.

A key for successful risk analysis is complete and accurate data for the generation of the system models used by the analysis tools. Most of the current generation of risk analysis tools depends on surveys filled out by users, system operations personnel, and analysts to acquire the data for development of the system model used for the analysis. Alternatively, active network scanning may be used to test various vulnerabilities against system components. Textual or survey-based knowledge solicitation techniques are labor intensive and potentially tedious for the analyst. Many of the existing tools reuse the same information to analyze different aspects of the system security. A centralized repository of modeling data could provide a basis for shared inputs among existing tools. This repository could be used to generate data sets for use by risk analysis tools, allowing multiple tools to be run against the same system without separate input activities, reducing the possibility of operator error. The use of multiple risk analysis reasoning engines, or backends, would allow various aspects of the system to be analyzed without the cost of developing one tool to perform all types of analysis. Integration of the information and the resulting informed assessments available by applying multiple tools could produce a more robust and accurate picture of a system's vulnerability posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison.

For the past two years, Harris Corporation has been conducting research for the Air Force Research Laboratory under the Network Visualization Tool (NVT) Program. The NVT concept defines a knowledge solicitation and translation framework for the risk assessment process. This framework incorporates a graphical description of a network topology, a central repository of modeling data, and report consolidation from multiple risk/vulnerability assessment tools into a single vulnerability assessment. Results are presented to a system user through a comprehensible, graphical

interface. The goal of this effort is to assess the feasibility of developing such a framework for a graphical risk analysis environment accommodating both existing and new risk analysis techniques.

The result of Network Visualization Tool effort is an initial vulnerability visualization and assessment environment, consolidating multi-source output into a cohesive capability within an open, standards-based architecture. This paper describes the NVT system architecture and its components, features and benefits of our approach, future research topics, and potential applications.

## II. System Overview

Under the Network Visualization Tool program, an innovative and unique vulnerability assessment framework that can accommodate changes to threat and technology environment and preserve the data from current risk analysis tools is being developed. The goal of this effort is to research, develop, test, and demonstrate an engineering prototype for a system vulnerability assessment framework that helps system architects identify security vulnerabilities and develop cost-effective countermeasures.

NVT provides a flexible, extensible, and maintainable solution. The NVT prototype isolates factual information about a system from the reporting and processing capabilities of individual vulnerability assessment tools. No single vulnerability assessment tool can adequately address all components of a comprehensive system architecture. A monolithic assessment system is difficult to evolve with the dynamic nature of threat and technology. NVT allows multiple tools to share data, and then fuses their results to provide a concise picture of a network's security posture to an NVT user, as illustrated in Figure 1. Our objective was to develop a prototype system security engineering tool that:

- Functions as a design tool to identify vulnerabilities in an architecture before the architecture is built and help enforce good security design principles

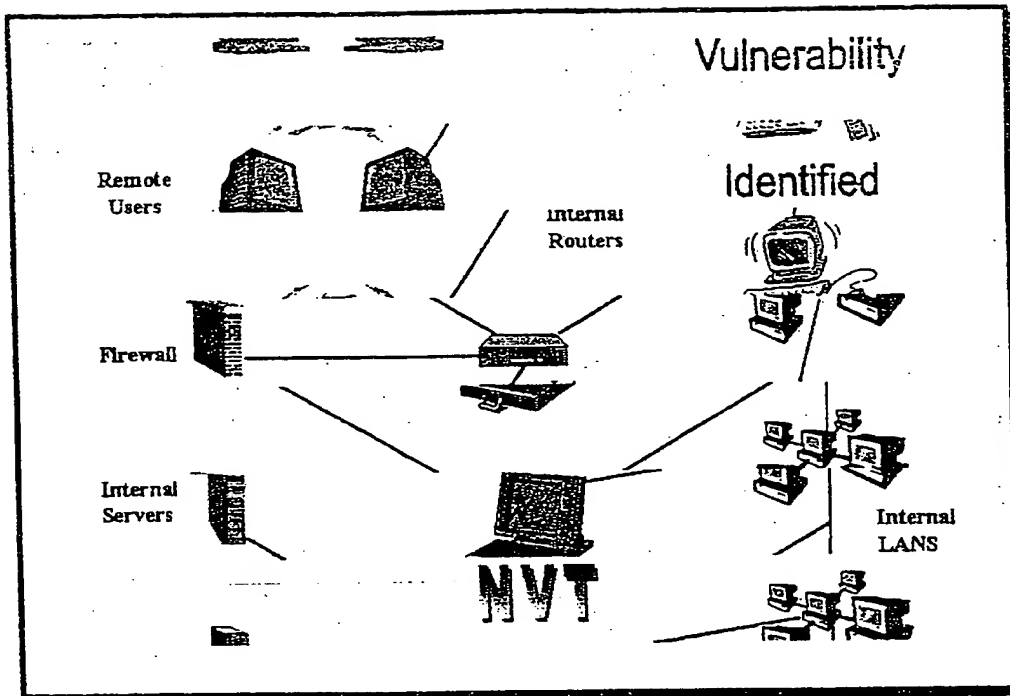


Figure 1. NVT Fuses the Results of Multiple Risk Analysis Tools to provide a Single, Comprehensive Network Security Posture Report.

- ❑ "Snapshots" a system and its vulnerabilities, enabling comparison of how risk evolves over the system lifecycle
- ❑ Applies static vulnerability databases from a variety of sources
- ❑ Applies legacy risk analysis tools and threat models
- ❑ Correlates information from various risk models/tools into an understandable picture of the system's vulnerabilities
- ❑ Allows what-if analysis to facilitate trade off analysis between security, functionality, performance, and availability
- ❑ Provides an easy to use way to specify the relevant characteristics of a system design

Our vision for a system security engineering tool facilitating system vulnerability assessment incorporates a single, graphical representation of a system. This system representation is provided to multiple risk/vulnerability assessment tools and vulnerability data or

knowledge bases, resulting in a single, consolidated input to multiple tools. A Fuzzy Expert System applies the unique correlation technology of *FuzzyFusion™* to combine the results from the various tools into a single, clear, unified report. The architecture concept is illustrated in Figure 2.

The NVT prototype is implemented on an Intel Pentium PC platform running Windows NT. This platform was selected as a low cost solution supporting a large variety of assessment tools. The initial tool suite employs a number of COTS/GOTS capabilities including:

- ❑ HP OpenView, for network automatic discovery or manual network modeling.
- ❑ ANSSR, a GOTS network system analysis tool developed by MITRE.
- ❑ RAM, NSA's risk assessment methodology, implemented in the DPL-f decision support programming language.
- ❑ ISS Internet Scanner, a scanning vulnerability tool suite.

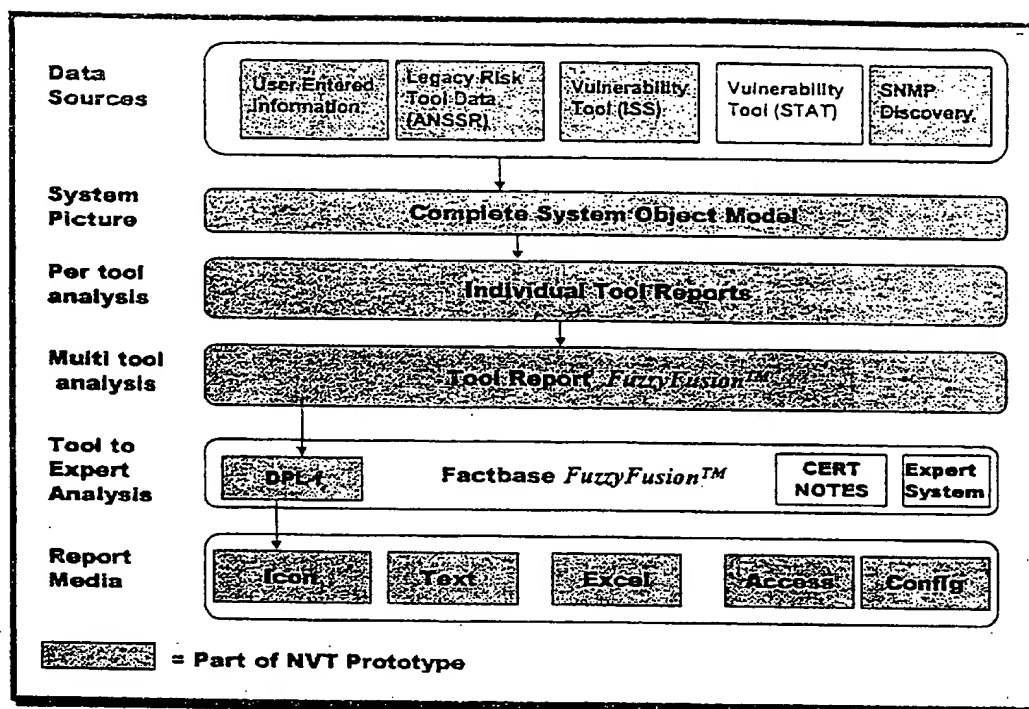


Figure 2. The NVT Vulnerability Assessment Tool Architecture Concept.

With supporting compilers and display capabilities, NVT represents the integration of 12 COTS packages into a cohesive risk assessment capability.

## II.1 System Architecture Data Entry

NVT is based on the concept of a knowledge solicitation framework that incorporates a graphical description of a network topology. This topology is used for capture of network attributes, and is subsequently analyzed for security vulnerabilities. The knowledge solicitation portion of NVT applies modern network discovery capabilities and a graphical user interface. This improves the accuracy of the network model, provides a common network description for multiple risk analysis reasoning engines, and enhances the productivity of the system security analyst.

The NVT prototype automatically maps an existing network, or can be used for the manual entry of a network design. The prototype uses HP OpenView to graphically depict a network topology. As illustrated in Figure 3, once it has

been given the IP address of the default router for the network, NVT, through the use of OpenView, can search for computers and other devices attached to the network. It performs an active search, pinging possible IP addresses on the network, and adding whatever response information it receives to its network map. NVT also provides, through OpenView, a manual method to draw a proposed network with a graphical user interface that supports drag and drop. A System Security Engineer can rapidly define a given system architecture, including the security critical information. For example:

- A user can apply the manual entry capability to consider alternative designs as part of a trade study.
- A user may edit the properties of each node, providing additional details as required to provide complete logical network planning.
- A user can also represent an entire network on a map by using a subnetwork icon. A detailed map of the subnetwork can be linked to this icon and displayed by double clicking on the icon.

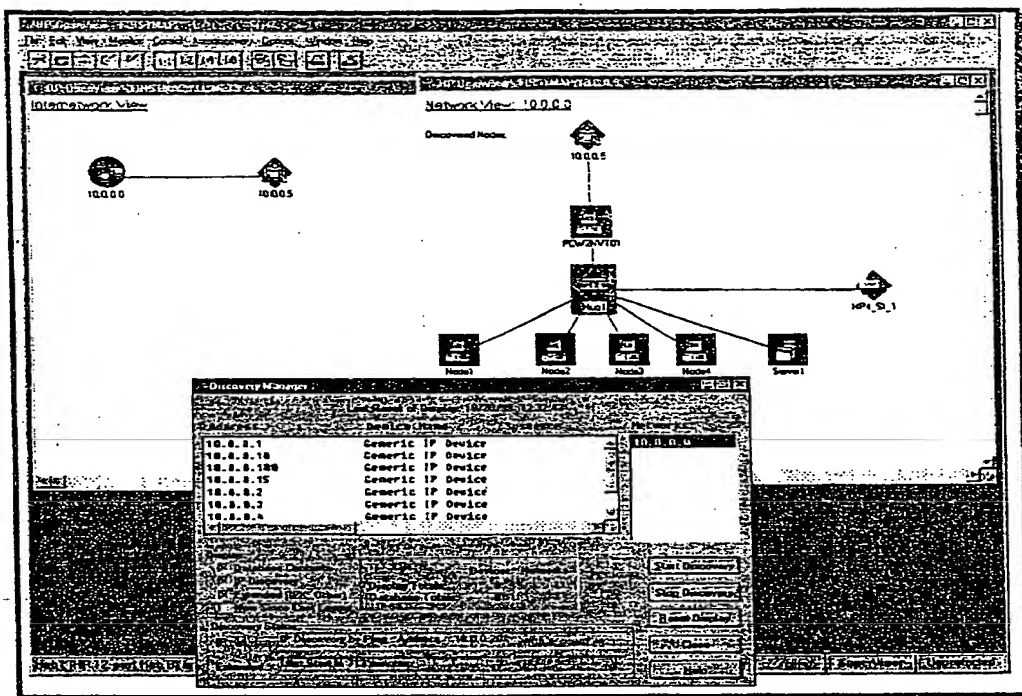


Figure 3. HP OpenView's Network Discovery Tools enable NVT users to Map an Existing Network for Further Security Analysis

Once the system description has been completed, the NVT prototype represents and stores the description in an object/class hierarchy. This single topological model supports the information needs of multiple reasoning (vulnerability/risk assessment) tools, as well as the *FuzzyFusion*<sup>TM</sup> of their results into a cohesive vulnerability/risk assessment. NVT translates this system representation into the appropriate format for each of the assessment tools employed. This single representation of a system simplifies the use of multiple tools, eliminating redundant data entry. It also provides the foundation for addressing the problem of incomplete data for a given vulnerability assessment tool, and for future knowledge negotiation capabilities.

## II.2 Risk Analysis Tool Selection

Under the Network Visualization Tool program, current COTS, GOTS and research vulnerability assessment and reasoning tools were surveyed to determine their capabilities and availability. Tools were categorized by the types of vulnerabilities assessed, and their functional

characteristics. Each tool was further evaluated on its data acquisition and output formats to determine how the information can be applied in the NVT engineering prototype implementation. The primary criteria were the operating system required by the tool, the capability of the tool to assess network environments, the data gathering methods used by the tool, and the risk types assessed by the tool. The vulnerability assessment and reasoning tools have to be able to run in the NVT prototype's operational environment (a PC with Windows NT).

A primary purpose of the NVT prototype is to demonstrate a framework with the flexibility to integrate and interactively use multiple existing vulnerability assessment and reasoning technologies. In order to demonstrate the proof of concept of integrating and interactively using multiple existing vulnerability assessment and reasoning technologies within program restrictions, a representative sample of tools was selected for inclusion in NVT. As a result of the tool survey, ANSSR, RAM, and ISS Internet Scanner were selected for inclusion in NVT.

Table 1. Capabilities Summary for the NVT prototype's Initial Set of Analysis Tools		
Selected Tool	Functional Capabilities	
ANSSR (Analysis of Networked Systems Security Risks) Mitre Corporation	<i>Passive data gathering</i> <ul style="list-style-type: none"> <li>- Model structure</li> <li>- Survey based data gathering</li> <li>- Network aware</li> </ul>	<i>Risk Type</i> <ul style="list-style-type: none"> <li>- Single Occurrence of Loss</li> </ul>
RAM (Risk Assessment Model) NSA	<i>Passive data gathering</i> <ul style="list-style-type: none"> <li>- Event tree</li> <li>- Prioritized attack list</li> </ul> <i>Risk Type</i> <ul style="list-style-type: none"> <li>- Mathematical model</li> <li>- Multiple risks/services</li> <li>- Event based over time</li> </ul>	<i>Extensible to Risk Type</i> <ul style="list-style-type: none"> <li>- Comparison of effectiveness of different designs</li> <li>- Not limited to computers/networks</li> <li>- Optimization of system/cost benefit analysis</li> </ul>
ISS Internet Scanner Internet Security Systems (ISS) Corporation	<i>Active data gathering</i> <ul style="list-style-type: none"> <li>- Scans network for hosts, servers, firewalls, and routers</li> <li>- Assesses security and policy compliance of networks, operating systems, and software applications</li> </ul>	<i>Risk Type</i> <ul style="list-style-type: none"> <li>- Computer Network Compliance Report (snapshot in time)</li> </ul>

These three tools met the requirements and provided the greatest diversity of functional capabilities, as shown in Table 1. The selected tools represent the greatest diversity of characteristics with the fewest expected integration risks.

The RAM model has been incorporated into a COTS tool, the DPL-f programming language for decision support, developed by Applied Decision Analysis, Inc., a subsidiary of PriceWaterhouseCoopers, LLC. This provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets, and graphical portrayal of risk over time.

### II.3 Output Report Correlation and Generation

None of the above tools take an aggregate snapshot approach to the system, with a "drill down" or layered approach to address risk at various layers (network, platform, database, etc.) of the system. Using multiple risk analysis tools would allow various aspects of the system to be analyzed for vulnerabilities without the cost of developing one tool to perform all types of analysis. To provide a more comprehensive vulnerability assessment of a system than any one tool could provide, the outputs of the various tools must be integrated and fused into a

single, concise report. This would provide greater assistance to system designers analyzing alternatives among security risk, system performance, and mission functionality.

Under the Network Visualization Tool effort, we investigated technologies that would support our goal of integrating and fusing the results from multiple vulnerability analysis applications. By examining the variety of current COTS and GOTS products, and the variety of inputs and outputs those products require, it became apparent that fuzzy decision technology offered the most flexible solution to our problem. Our focus on fuzzy decision methodologies as our technology foundation was based on an analysis of a variety of technologies, including Expert Systems, Databases Systems, Data Fusion, Neural Networks, Fuzzy Logic, and Fuzzy Expert Systems. The later is based on the premise that multi-criteria, multi-expert decision making can lead to a best-fit answer. Primary benefit of a fuzzy reasoning system is its ability to use and assimilate knowledge from multiple sources. We believe that fuzzy expert system technology is applicable because:

- ☐ An expert exists for each tool that we wish to include in the system
- ☐ The problem itself is fuzzy; it has ambiguities and often partial information

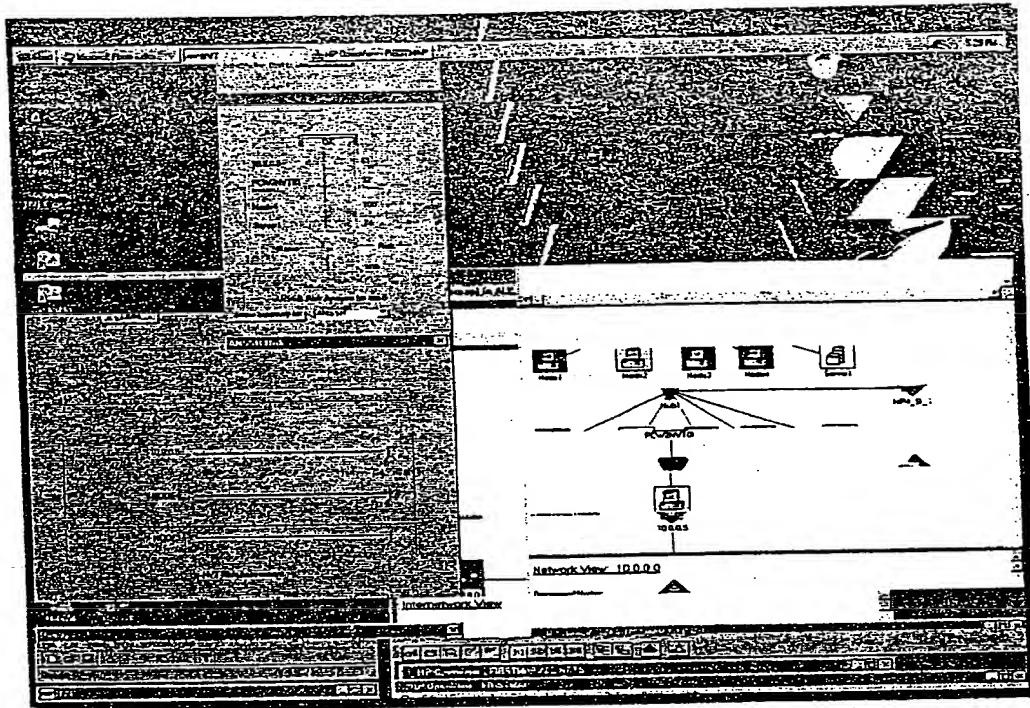


Figure 4. NVT leverages Existing Vulnerability Assessment Tools to present a Single, Cohesive Risk Picture.

- We can incrementally learn and apply new technologies as the system grows
- We believe we can identify valid membership functions for the mapping of data to concept and concept to knowledge

As a result of our research of existing technologies, Harris has developed **FuzzyFusion™** technology to combine the results of multiple vulnerability assessment/risk analysis tools into a unified report. **FuzzyFusion™** combines the techniques of fuzzy logic, fuzzy expert systems and data fusion. **FuzzyFusion™** incorporates Level 2 data fusion, since our data is already aligned. We have an established network model and operator environment, and need to establish the relationship between the network model and the findings of the risk analysis tools. Real world measurements are captured in fuzzy logic. The reasoning concepts from data fusion are used to establish relationships among the network model, vulnerability findings from the various

tools, and the knowledge of network security experts. **FuzzyFusion™** is accomplished through the use of a fuzzy expert system, which combines the outputs of the various tools, user concerns about system risks and vulnerabilities, and expert understanding of the results of each tool and how these fit into the larger information system security picture.

Output of the concise assessment can be provided to the NVT user through multiple means and in various degrees of detail, as illustrated in Figure 4. The graphical network map of a system can be color-coded to provide a visual indication of where the greatest risks are located. In Figure 4, the node with the greatest associated risk is colored red. Less severe risks are colored yellow. A pop-up slider window can also be utilized to indicate the top *N* risks, and their severity. Further details, such as text reports and spreadsheet analyses, can be accessed by drilling down through the layers of information.

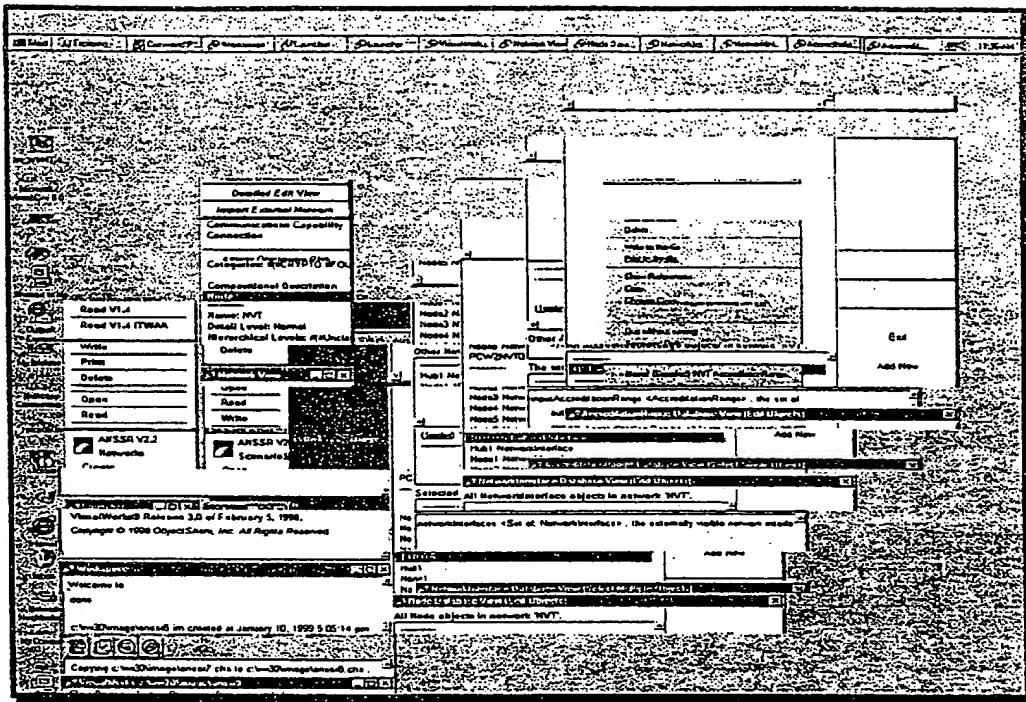


Figure 5. Entering System Information into the Interface for ANSSR is a Manually Intensive Process.

### III. Features & Benefits of NVT

The result of the NVT Program is a prototype demonstrating a comprehensive vulnerability profile based on the user defined acceptable risk of compromise to a given system. End users have a simple expression of the *vulnerability posture* of a given system or system design, and are capable of performing "what if" analysis for functionality, performance, and countermeasure trades.

The primary advantage of the NVT prototype is that it provides a flexible, modular, extensible approach to vulnerability assessment. This innovative design accommodates multiple risk assessment techniques, but only requires single entry of the system description (through auto discovery or manual entry of a model), which is a significant benefit to the System Security Engineer. Figure 5 illustrates the interface to ANSSR, which supports a character based GUI when it is used as a stand-alone tool. As the number of windows and menus suggests, entry of information into the tool is a manually intensive exercise. One of the benefits of NVT

is that it automates providing the required system information to the various vulnerability assessment tools, allowing each tool to use only the input data it requires. NVT eliminates the manually intensive operations associated with legacy assessment tools, and preserves existing user investment in legacy methodologies. NVT also provides a mechanism to correlate information among tools. Information solicited from the user for any single tool is shared among all tools. Legacy vulnerability assessment tools and databases can be reused, and their results used in conjunction with alternate risk models.

NVT was designed to be an affordable vulnerability assessment environment. Many monolithic risk assessment tools require high performance Unix platforms and cost over \$40,000 per copy of each tool. The NVT prototype is being developed on a Windows NT-based Pentium platform. Our initial tool suite reflects a desire to be economical and pragmatic in tool selection. Three COTS/GOTS vulnerability assessment tools, are incorporated into the framework: ANSSR, DPL-f, and ISS Internet Scanner. Costs for the runtime licenses

of COTS products currently employed within the NVT prototype along with a suitable NT workstation are approximately \$30,000.

The modular, extensible system design for NVT ensures ease of technology transition and integration as new vulnerability tools and technology vulnerabilities come to market. This modularity also preserves user legacy models, and allows each user to select the tools most appropriate for his environment and needs. This model also allows a user to preserve his corporate investment. For example, if an organization already employs active scanning technology, the tool can be integrated into the NVT framework with little difficulty. This provides a new source of input (the existing tool), and makes new processing elements (additional risk assessment tools) available to the enterprise.

#### IV. Future Research

The basic foundation of NVT provided valuable experience in risk analysis tool integration and correlation technologies. Future research and development efforts would benefit from feedback from System Security Engineers using the NVT prototype as a tool to:

- Identify vulnerabilities and enforce good security design principles
- "Snapshot" a system and its vulnerabilities, and compares how risk evolves over the system lifecycle
- Correlate information from various risk tools in an understandable graphical vulnerability analysis
- Support hypothetical analysis, facilitating architecture choices among security, functionality, performance, and availability
- Provide rapid specification of the relevant characteristics of a system design

Beyond the efforts conducted under the initial NVT Program, further research is needed to improve the *FuzzyFusion*<sup>TM</sup> used to combine outputs from various risk analysis tools into a unified report. In addition, we have identified

new functionality to incorporate into result analysis, including:

- **Temporal based reasoning** – accounts for the time required to exploit a known vulnerability as part of the system assessment process. It enables a user to perform a vulnerability assessment that takes into account the time required to exercise a given vulnerability. For example, if time required to penetrate/compromise a node exceeds the timeline for a mission, then the threat is minimal.
- **Vulnerability thresholding** – minimizes continued computation when an aggregate vulnerability level in a given system or segment exceeds a user defined limit, allowing the user to define his own vulnerability tolerance. It eliminates possibly computationally intensive search trees when a sufficiently lethal vulnerability is located, or when a large number of vulnerabilities are identified. It allows the user to define his vulnerability tolerance level, and supports tailorable definitions of acceptable levels of vulnerability.
- **Reasoning with uncertainty or incomplete data information** – provides the user with some answer, the best that is available with the information available.
- **Vulnerability trade-off visualization techniques** – allow the user to easily perform what-if analysis and experimentation among performance, functionality, and countermeasures. It enables the user to readily understand the trade-offs among desired capabilities.

This functionality will allow NVT to more accurately reflect the human decision making process. Further, it will support a more robust, systems orientation towards vulnerabilities, accommodating consideration of application and platform vulnerabilities as well as network vulnerabilities.

#### V. Potential Applications

The NVT program has developed foundation technology that can be applied to three distinct

related problem domains: security risk assessment, security modeling, and security administration. Our initial research, as well as this paper, was directed at the security risk assessment problem domain. NVT could also be integrated with existing network modeling tools to provide a security perspective to network modeling environments. As a security administrator's toolset, NVT could be an integration platform for administrative tools such as password dictionaries, to provide an operationally oriented security assessment capability.

*This research was funded under the Network Visualization Tool (NVT) program for U.S. AFRL/IFGB, contract #F30602-96-C-0289. U.S. Government Publication Release Authority: Dwayne P. Allain or Peter J. Radesi.*

## References

1. *Computers in Security*. Charles P. Pfleeger. Prentice Hall PTR. Upper Saddle River, NJ. 1997.
2. "Sniffing Out Network Holes". Leslie O'Neil and Joe Scambray. *INFOWORLD*. February 8, 1999. Pp. 74-82.
3. *Analysis of Networked Systems Security Risks (ANSSR) Assessment Tool, Version 2.2, User's Manual*. D. J. Bodeau and F. N. Chase. The MITRE Corporation. Bedford, MA.
4. "ANSSR: A Tool for Risk Analysis of Networked Systems". D. J. Bodeau, F. N. Chase, and S. G. Kass. *Proceedings of the 13<sup>th</sup> National Computer Security Conference*. October 1990.
5. "A Practitioner's View of CRAMM". Norman Truman. Gamma Secure Systems Limited.  
<http://www.gammass1.co.uk/topics/hot5.htm>  
1. September 1997.
6. *DPL-f User Manual*. Applied Decision Analysis LLC. 1999.
7. *ISS Internet Scanner User Guide for Windows NT*. Internet Security Systems (ISS). Atlanta, GA. 1997.
8. *HP OpenView for Windows: Workgroup Node Manager User's Guide*. Hewlett Packard. Cupertino, CA. 1998.
9. *HP OpenView: Professional Suite Getting Started Guide*. Hewlett Packard. Cupertino, CA. 1998.
10. "L-3 Network Security Expert 3.0". Product review, *SC Magazine* (Information Security News).  
<http://www.infosecnews.com/13/13.html>.
11. *Network Visualization Tool Program - Final Scientific & Technical Report*. R. R. Henning, K. L. Fox, J. T. Farrell, C. C. Miller, E. P. Meijer. Harris Corporation. Melbourne, FL. June 1999.

## Author's Biography

Ronda Henning is the senior Secure Systems Engineer for Harris Corporation, Government Communications Systems Division; a Melbourne, Florida based international communications and electronics company. Ms. Henning currently leads the Information Assurance center of excellence, an interdisciplinary engineering group responsible for information assurance technology research and development as well as assurance technology insertion large scale systems integration opportunities. A member of the Harris Engineering Process Group, Ms. Henning developed the Harris Secure Systems Engineering Guidebook, and was a founding member of the National Security Agency (NSA)/Industry consortium responsible for the System Security Engineering Capability Maturity Model (SSE-CMM). Prior to her employment at Harris, Ms. Henning was a deputy branch chief of information security research and development at the National Security Agency. A Certified Information Systems Security Professional (CISSP), she holds an M.B.A. from the Florida Institute of Technology, an M.S. in Computer Science from Johns Hopkins University, and a B.A. from the University of Pittsburgh.

# The Network Vulnerability Tool — A System Vulnerability Visualization Architecture

**HARRIS**

---

**The Network Vulnerability Tool —  
A System Vulnerability Visualization Architecture**

Kevin L. Fox, Ph.D.  
407-684-8011  
kfox@harris.com

Ronda R. Henning  
407-684-6009  
rhenning@harris.com


**HARRIS**

**Network Visualization Tool Program**

- AFRL-funded research program with 2 goals:
  1. Investigate:
    - The feasibility of a common risk assessment and vulnerability detection architecture
    - Enhanced usability, productivity, and system coverage
  2. Define techniques to promote:
    - enhanced knowledge solicitation
    - normalized, shared system representation
    - application of data fusion techniques to risk and vulnerability reporting
    - comprehensible reporting mechanisms for results interpretation

**HARRIS**

**User's Perspective**




- "I don't know what's on my network"
- "The last risk assessment was done 15 years ago"
- "I don't know if I can connect my legacy systems in transition"
- "How do I know if I've fixed all the systems"
- "What is an acceptable risk?"

**HARRIS**

**The Risk Tool Landscape**

- Monolithic, proprietary environments
- Difficult to incorporate new threats or technologies
- Multiple tools with multiple system representations
  - from users and scanning technology
  - no reuse or information sharing
- Diverse, single solution tools
  - vulnerability scanners
  - systemic risk assessment
  - paper risk assessments
  - legacy tool suites



**HARRIS**

**Concept of Operations**

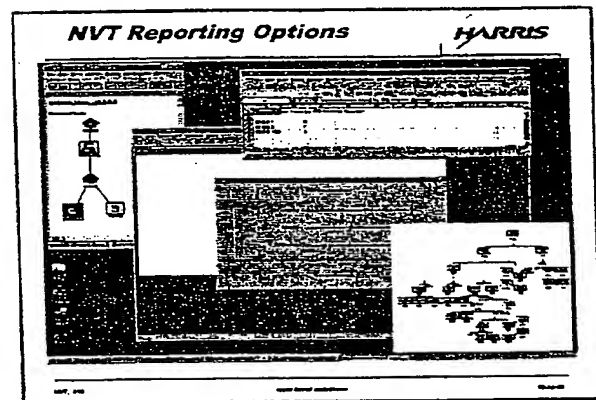
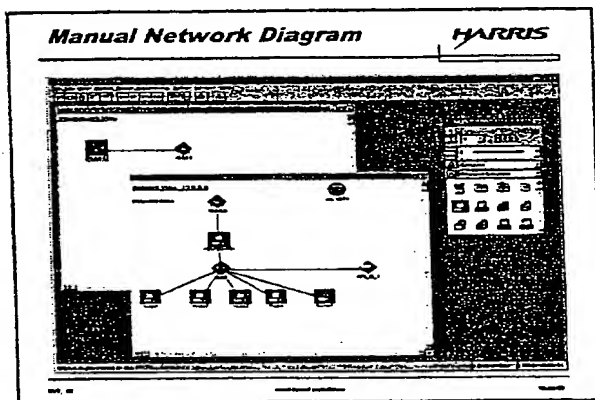
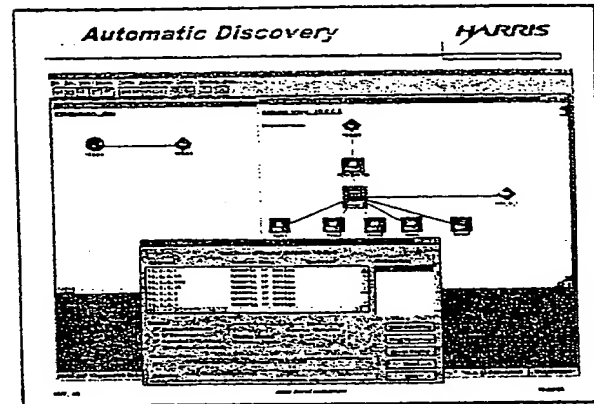
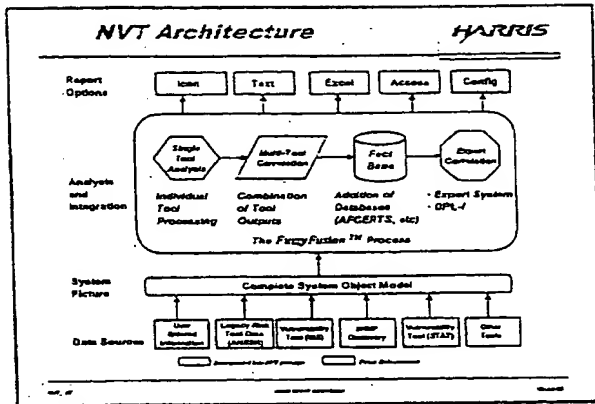
System Designers	Security Officers
<ul style="list-style-type: none"> <li>• Mitigate/define security architecture</li> <li>• Architecture options analysis</li> <li>• Stop problems before they become problems</li> <li>• Fulfill requirement for a system risk analysis</li> <li>• Use as a Design tool during system development</li> </ul>	<ul style="list-style-type: none"> <li>• Deployed systems               <ul style="list-style-type: none"> <li>• Determine system risk posture</li> <li>• Determine how risk evolves over the system life cycle</li> </ul> </li> <li>• Legacy systems               <ul style="list-style-type: none"> <li>• Measure associated risk</li> <li>• Key to Infrastructure modernization</li> <li>• Understand and accept the implications of connectivity</li> </ul> </li> <li>• Use during the life cycle to "snapshot" a system's risk posture.</li> </ul>

**HARRIS**

**Risk Analysis Tools**

- Three distinct risk/vulnerability analysis tools were integrated in a proof-of-concept prototype
  - ANSSR was selected as a prime example of a legacy reasoning engine
  - ISS Internet Scanner was selected as an example of a "live" vulnerability tool
  - Risk Assessment Methodology (RAM) was selected for large scale, highly complex problems
    - Replaced by DPL-f
- HP Open View used for SNMP Network Management Mapping Environment

# The Network Vulnerability Tool — A System Vulnerability Visualization Architecture



**NVT Program Conclusions** **HARRIS**

- Demonstrated an initial proof-of-concept
  - Can combine multiple assessment tools with different modes of operation to provide a more complete picture
  - Fuzzy Logic and Data Fusion concepts/technologies are viable for use in result integration
  - Use multiple tools to fill in or resolve missing data required by other tools
- Primary advantages of NVT prototype
  - Provides a flexible, modular, extensible approach to vulnerability assessment
  - Accommodates multiple assessment techniques, BUT only requires single entry of network description
  - Preserves investment in legacy methodologies/tools, but reduces associated labor

**Conclusions - Continued** **HARRIS**

- The NVT prototype was designed to be an affordable vulnerability assessment environment
  - Developed on Windows NT, Pentium platform
  - Costs for runtime licenses of COTS products currently employed along with a suitable workstation - \$30K
  - Design facilitates incorporation of other vulnerability assessment technologies
    - Incorporation of new tools into NVT environment < 1 min
    - Time then required to modify FuzzyFusion™
    - Select tools most appropriate for a given environment
    - Preserves investment already in place

# The Network Vulnerability Tool — A System Vulnerability Visualization Architecture

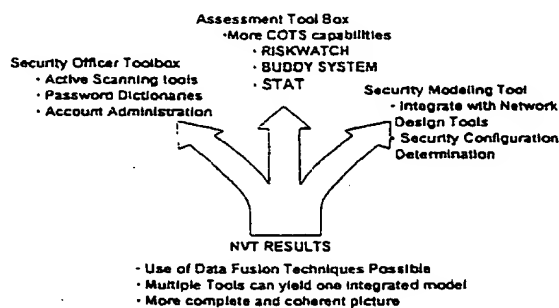
## Future Research Topics

HARRIS

- Temporal-Based Reasoning
  - Enables analyst to perform an assessment that accounts for time required to exploit a known vulnerability
- Vulnerability Thresholds
  - Minimizes continued computation when an aggregate vulnerability level in a given system exceeds a user-defined limit
  - Eliminates possibly computationally intensive search trees when a sufficient lethal vulnerability is located
  - Allows a user to define a vulnerability tolerance level
- Vulnerability Trade-off Visualization Techniques
  - Allow the user to perform what-if analysis among performance, functionality and countermeasures
- Incorporate Static Vulnerability Database(s)

## Possible Directions

HARRIS



Questions?

**This Page Blank (uspto)**